UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/072,683 | 02/08/2002 | Nir Zuk | 0023-0209 | 2532 |

44987 7590 09/28/2011

HARRITY & HARRITY, LLP
11350 Random Hills Road
SUITE 600
FAIRFAX, VA 22030

| EXAMINER | |
|---|---|
| RAHMAN, MOHAMMAD L | |
| ART UNIT | PAPER NUMBER |
| 2438 | |
| MAIL DATE | DELIVERY MODE |
| 09/28/2011 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/072,683 | ZUK ET AL. | |
| | Examiner | Art Unit | |
| | MOHAMMAD RAHMAN | 2438 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *06/30/2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

5)☐ Claim(s) *See Continuation Sheet* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☐ Claim(s) *1-7,10,12,13,15-18,21,23-25,27,31,32,37,38,40-45,55-58,60-63,65 and 66* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/09/2008, 06/28/2010*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Disposition of Claims: Claims pending in the application are 1-7,10,12,13,15-18,21,23-25,27,31-32,37-38,40-45,55-58,60-63,65 and 66.

***Continued Examination Under 37 CFR 1.114***

A request for continued examination under 37 CFR 1.114 was filed in this application after a decision by the Board of Patent Appeals and Interferences, but before the filing of a Notice of Appeal to the Court of Appeals for the Federal Circuit or the commencement of a civil action. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 06/30/2011 has been entered.

***Response to Arguments***

Independent claims have been amended to incorporate new limitations as "each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to one or more of the packet flow descriptor". Applicants argued that the newly added limitation is not taught by the prior arts on the record.

While applicant has changed the scope of the claims by way of amendments, the examiner continues to rely on prior art on the record and so will address applicant's arguments below for clarifying the teaching of prior art.

Applicants have not clearly defined the communication session in the claim. To clearly address the applicants recited limitation, examiner has carefully read the specification and specification discloses (PgPub paragraph. 0094) that "the packet flow descriptors addressed by each key consist of information about each specific packet flow, each packet flow is associated to a session, such as TELNET session, FTP session, and HTTP session." Copeland et al. (prior art on the record) teaches, [0050], "***The flow data structure stores collected flow information such as***

***IP addresses. The flow data structure also stores time and other related packet information from the packet header***." It is well-known and can be found any network textbook that packet header contains protocol information [on networks that carry multiple types of information, the protocol defines what type of packet is being transmitted: e-mail (SMTP), Web page (HTTP), streaming video (RTSP)]. However, ***Copeland further teaches in paragraph 0034, 0038, data flow contains data packet that can include FTP, SMTP, HTTP communications***. It is obvious that each packet flow in the flow data structure in Copeland points to one of the communication sessions and each of the communication session points to one or more packet flow).

Applicants present no further arguments.

The Examiner is attempting to clarify the teachings of the prior art reference and how it reads on the claims. In order for the applicant to have ample opportunity to provide perusasive arguments and /or amendment of the claims to overcome the prior art of record, THIS ACTION IS MADE NON-FINAL.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 27, 31-32, 37-38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Independent claim 27 is directed towards "a system" and claim element "a software module to inspect/drop/forward/group" is a limitation that invokes 35 U.S.C. 112, sixth paragraph. Claim limitation clearly recites software module, therefore directed towards 'software

per se', non-statutory. Dependent claims 31-32, 37-38, 40 do not cure the deficiencies set for the above.

Applicant may:

(a) Amend the claim so that the claim limitation will no longer be interpreted as a limitation under 35 U.S.C. 112, sixth paragraph; or

(b) Amend the written description of the specification such that it expressly recites what structure, material, or acts perform the claimed function without introducing any new matter (35 U.S.C. 132(a)).

If applicant is of the opinion that the written description of the specification already implicitly or inherently discloses the corresponding structure, material, or acts so that one of ordinary skill in the art would recognize what structure, material, or acts perform the claimed function, applicant should clarify the record by either:

(a) Amending the written description of the specification such that it expressly recites the corresponding structure, material, or acts for performing the claimed function and clearly links or associates the structure, material, or acts to the claimed function, without introducing any new matter (35 U.S.C. 132(a)); or

(b) Stating on the record what the corresponding structure, material, or acts, which are implicitly or inherently set forth in the written description of the specification, perform the claimed function. For more information, see 37 CFR 1.75(d) and MPEP §§ 608.01(o) and 2181.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

***Claims 1-7, 10, 12-13, 15-17,21, 23-25, 31, 37-38 and 40-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) and Gleichauf et al. (6,324,656) in view of Nikander et al. (6,253,321) in view of Copeland, III (2003/0105976).***

**Regarding claim 1, 24**, (currently amended) Gleichauf discloses a method / a system comprising : at least one sensor, implemented in hardware, where the at least one sensor is to

(***e.g. col. 2, lines 42-47, "a method and system for adaptive network security using intelligent packet analysis"; fig. 2,3***)

reassembling / reassemble a plurality of TCP packets in network traffic into a TCP stream (***i.e. TCP stream reassembly, col. 6, lines 39-40 , to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer***);

inspecting / inspect the TCP stream to detect information indicative of a security breach (***e.g. col. 3, lines 1-4***) ; where inspecting the TCP stream to detect information indicative of a security breach comprises / where the at least one sensor further is to (***e.g. col. 2, lines 50-55***): storing / store a plurality of protocol specifications supported by the network in a protocol database, querying / query the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (***col. 6, lines 31-33; col. 8, lines 20-35***).

Gleichauf (6,324,656) also discloses inspecting the TCP stream to detect information indicative of a security breach comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (***Fig. 3B; col. 6, lines 32 – col. 7, line 5***).

Gleichauf does not explicitly disclose dropping / drop a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding / forward a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches.

Nikander is relied on for the teaching of dropping / drop a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding / forward a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches (***Nikander, col. 4, lines 41-45***).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf (6,499,107 and 6,324,656) and Nikander do not specifically disclose grouping / group the plurality of TCP packets into packet flows and communication sessions; storing / store information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to one or more of the packet flow; searching / where, when inspecting the TCP stream, the at least one sensor further is to search for a network attack identifier in the TCP stream based on the packet flow descriptors and communication sessions associated with the TCP stream.

Copeland is relied on for the teaching of grouping the plurality of TCP packets into packet flows and communication sessions (***Copeland, paragraphs 0039; 0050***); storing information

regarding the packet flows in packet flow descriptors where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to one or more of the packet flow (***Copeland, paragraph 0050, "The flow data structure stores collected flow information such as IP addresses. The flow data structure also stores time and other related packet information from the packet header."*** **Applicants do not clearly define about the communication session in the claim but disclose in the specification (Para 0094) that the packet flow descriptors addressed by each key consist of information about each specific packet flow, each packet flow is associated to a session, such as TELNET session, FTP session, and HTTP session.** It is well-known and can be found any network textbook that packet header contains protocol information [on networks that carry multiple types of information, the protocol defines what type of packet is being transmitted: e-mail (SMTP), Web page (HTTP), streaming video (RTSP)]. However, Copeland further teaches in paragraph 0034, 0038, data flow contains data packet that can include FTP, SMTP, HTTP communications. It is obvious that each packet flow in Copeland points to one of the communication session and each of the communication session points to one or more packet flow) and searching for a network attack identifier in the TCP stream based on the packet flow descriptors and communication sessions associated with the TCP stream (***Copeland, paragraphs 0051, 005, 0081-0083, 0172***).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of grouping the plurality of TCP packets into packet flows and sessions in the system of Gleichauf and Nikander, as Copeland teaches so as to effectively determine if the traffic data appears to be legitimate or possible suspicious activity.

**Regarding claim 2, 12, and 15**, (currently amended) Gleichauf further discloses the method of claim 1, where inspecting the TCP stream to detect information indicative of the

security breach comprises inspecting the TCP stream for protocol irregularities (***Gleichauf, col. 6, lines 36-42***).

**Regarding claim 3, 13, and 16-17**, (currently amended) Gleichauf further discloses the method of claim 1, where inspecting the TCP stream to detect information indicative of the security breach comprises searching the TCP stream for attack signatures (***Gleichauf, col. 1, lines 29-31***).

**Regarding claim 4, 31**, (currently amended) Gleichauf further discloses the method of claim 3, where searching the TCP stream for attack signatures comprises using stateful signature detection / the system of claim 24, where the at least one sensor further is to: detect information indicative of the security breach based on a stateful signature (***Gleichauf, col. 6, lines 45-52***).

**Regarding claim 5,** (currently amended) Gleichauf further discloses the method of claim 1, where inspecting the TCP stream to detect information indicative of the security breach comprises using a plurality of network intrusion detection methods (***Gleichauf, col. 6, lines 66-67***).

**Regarding claim 6**, (currently amended) Gleichauf further discloses the method of claim 5, where the plurality of network intrusion detection methods comprises at least protocol anomaly detection (***Gleichauf, col. 6, lines 36-42***).

**Regarding claim 7**, (currently amended) Gleichauf further discloses the method of claim 5, where the plurality of network intrusion detection methods comprises at least signature detection (***Gleichauf, col. 6, lines 43-45***).

**Regarding claim 10**, (currently amended) Gleichauf-Nikander-Copeland combination further teaches the method of claim 1, further comprising searching the packet flow descriptors for traffic signatures (***Copeland, Page 6, paragraph [0070]***).

**Regarding claim 21, 38**, (currently amended), Gleichauf discloses the method of claim 3, where searching the TCP stream for attack signatures comprises / the system of claim 24, where the at least one sensor further is to: querying / query a signatures database to identify determine whether there are matching attack signatures in the TCP stream (***Gleichauf, col. 6, lines 45-52; col. 5, lines 36-42***).

**Regarding claim 23, 25,** (currently amended) Gleichauf discloses the method of claim 1, further comprising reconstructing the plurality of TCP packets from a plurality of packet fragments / the system of claim 24, where the at least one sensor further is to reconstruct a plurality of packet fragments into the plurality of TCP packets (***Gleichauf, col. 6, lines 39-40***).

**Regarding claim 37**, (currently amended) Gleichauf further teaches the system of claim 24, where the protocol specifications comprise specifications of one or more of: a TCP protocol; an HTTP protocol; a SMTP protocol; a FTP protocol; a NETBIOS protocol; an IMAP protocol; a POP3 protocol; a TELNET protocol; an IRC protocol; a RSH protocol; a REXEC protocol; or a RCMD protocol (***Gleichauf, Fig. 3B***).

**Regarding claim 40**, (currently amended) Gleichauf discloses the system of claim 24, further comprising: at least one processor to:

collect a plurality of security logs and alarms recording information about security breaches found in the TCP stream (***Gleichauf, col. 7, lines 1-5***); store a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented (***Gleichauf, col. 5, lines 33-42***); distribute a routine for distributing the network security policy to one or more gateway points in the network (***Gleichauf, Fig. 2. element 20***); and update routine for updating the protocol database and a signatures database (***Gleichauf, col. 9, lines 7-13***).

**Regarding claim 41**, (currently amended) Gleichauf-Nikander-Copeland combination further teaches the system of claim 24, further comprising a graphical user interface to display a routine for displaying network security information to network security administrators; and a routine for specifying a network security policy (***Copeland, page 11, paragraph [0182]***).

***Claims 18, 27 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) and Gleichauf et al. (6,324,656) in view of Nikander et al. (6,253,321) in view of Copeland, III (2003/0105976) and further in view of Alexander et al. (2004/0258073).***

**Regarding claim 18, 27**, (currently amended) Gleichauf discloses a method / a system comprising (***e.g. col. 2, lines 42-47, "a method and system for adaptive network security using intelligent packet analysis"; fig. 2, 3***):

reassembling / a TCP reassembly software to reassemble a plurality of TCP packets into a TCP stream (***i.e. TCP stream reassembly, col. 6, lines 39-40 , to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer***);

inspecting / a software module to inspect the TCP stream to detect information indicative of a security breach (***e.g. col. 3, lines 1-4***);

Gleichauf (6,324,656) also discloses inspecting the TCP stream to detect information indicative of a security breach comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether

the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (***Fig. 3B; col. 6, lines 32 – col. 7, line 5***).

Gleichauf does not explicitly disclose dropping / a software module to drop a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach; forwarding / a software module to forward a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach;

Nikander is relied on for the teaching of dropping / a software module to drop a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach; forwarding / a software module to forward a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach (***Nikander, col. 4, lines 41-45***);

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping / a software module to drop a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding / a software module to forward a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf (6,499,107 and 6,324,656) and Nikander do not specifically disclose grouping / a flow manager software module to group the plurality of TCP packets into packet flows and communication sessions, storing / store information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to a plurality of the packet flow

descriptors; and where inspecting the TCP stream to detect information indicative of the security breach further comprises / where the software module to inspect the TCP stream is to: searching / to search for a network attack identifier in the TCP stream based on the packet flow descriptors and the communication sessions associated with the TCP stream;

Copeland is relied on for the teaching of grouping / a flow manager software module to group the plurality of TCP packets into packet flows and communication sessions (***Copeland, paragraphs 0039; 0050***), storing / store information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to a plurality of the packet flow descriptors (***Copeland, paragraph 0050, "The flow data structure stores collected flow information such as IP addresses. The flow data structure also stores time and other related packet information from the packet header."*** **Applicants does not clearly define about the communication session in the claim but disclose in the specification (Para 0094) that the packet flow descriptors addressed by each key consist of information about each specific packet flow, each packet flow is associated to a session, such as TELNET session, FTP session, and HTTP session.** It is well-known and can be found any network textbook that packet header contains protocol information [on networks that carry multiple types of information, the protocol defines what type of packet is being transmitted: e-mail (SMTP), Web page (HTTP), streaming video (RTSP)]. However, Copeland further teaches in paragraph 0034, 0038, data flow contains data packet that can include FTP, SMTP, HTTP communications. It is obvious that each packet flow in Copeland points to one of the communication session and each of the communication session points to one or more packet flow); and where inspecting the TCP stream to detect information indicative of the security breach further comprises / where the software module to inspect the TCP stream is to (***detecting***

***information indicative of the security breach is already taught by Gleichauf in col. 2, lines 50-55***): searching / search for a network attack identifier in the TCP stream based on the packet flow descriptors and the communication sessions associated with the TCP stream (***Copeland, paragraphs 0051, 005, 0081-0083, 0172***);

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of grouping the plurality of TCP packets into packet flows and sessions in the system of Gleichauf and Nikander, as Copeland teaches so as to effectively determine if the traffic data appears to be legitimate or possible suspicious activity.

The combination of Gleichauf (6,499,107 and 6,324,656), Nikander and Copeland is teaches where grouping the plurality of TCP packets into the packet flows (***Copeland, paragraphs 0039; 0050***) and the communication sessions comprises storing information regarding the packet flows and the communication sessions (***Copeland, paragraph 0034, 0038 0050)*** but is silent on the capability of storing the information regarding the packet flows and the communication sessions in a hash table.

Alexander is relied on for the teaching of storing the information regarding the packet flows and the communication sessions in a hash table (i.e. computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type (***Alexander, page 3, paragraph [0027], protocol type has communication session information***).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type in the system of

Gleichauf (6,499,107 and 6,324,656), Nikander and Copeland as Alexander teaches so as to effectively performing packet filtering.

**Regarding claim 32**, (currently amended) Gleichauf-Nikander-Copeland-Alexander combination teaches the system of claim 27, further comprising a traffic signature detection software module to search_for searching the packet flow descriptors for traffic signatures (***Copeland, page 4, paragraphs [0047-0051]***).

***Claims 42-45, 55-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) in view of Nikander et al. (6,253,321) in view of Trcka et al. (6,453,345), and in further view of Copeland, III (2003/0105976)***

**Regarding claim 42,** (currently amended) Gleichauf discloses a system for detecting and preventing security breaches in a network, the system comprising (***e.g. col. 2, lines 42-47, "a method and system for adaptive network security using intelligent packet analysis"; fig. 2, 3***):

a network intrusion detection and prevention sensor located in a network gateway (***Gleichauf, fig. 2 and 3***), where the network intrusion detection and prevention sensor is reassemble a routine for reassembling a plurality of TCP packets into a TCP stream (***i.e. TCP stream reassembly, col. 6, lines 39-40, to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer***); inspect to detect information indicative of a security breach (***e.g. col. 3, lines 1-4***), where, when the network intrusion and detection sensor is to inspect the TCP stream, the network intrusion and detection sensor further is to wherein inspecting the TCP stream to

detect information indicative of a security breach (***e.g. col. 2, lines 50-55***)comprises: store a plurality of protocol specifications supported by a network in a protocol database, and query the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (***col. 6, lines 31-33; col. 8, lines 20-35***);

Gleichauf (6,324,656) also discloses inspecting the TCP stream to detect information indicative of a security breach comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (***Fig. 3B; col. 6, lines 32 – col. 7, line 5***).

Gleichauf does not explicitly disclose drop a TCP packet from the TCP stream if the TCP stream contains information indicative of the security breach; and forward a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of the security breach;

Nikander is relied on for the teaching of drop a TCP packet from the TCP stream if the TCP stream contains information indicative of the security breach; and forward a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of the security breach (***Nikander, col. 4, lines 41-45***);

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network

destination if the TCP stream does not contain information indicative of security breaches in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf and Nikander do not disclose a central management server and a graphical user interface.

Trcka discloses a central management server (***Trcka, col. 15, lines 13-21; Fig. 8, element 64***) to control the network intrusion detection and prevention sensor; and a graphical user interface to configure for configuring the network intrusion detection and prevention sensor (***Trcka, col. 13, lines 50-65***),

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ to use of having a central management server to control the network intrusion detection and prevention sensor and a graphical user interface for configuring the network intrusion detection and prevention sensor (col. 13, lines 50-65) in the system of Gleichauf and Nikander as Trcka teaches so as to detect and protect against security breaches, network failures and other types of data compromising events (col. 1, lines 10-15).

Gleichauf (6,499,107 and 6,324,656), Nikander and Trcka do not specifically disclose the network intrusion detection and prevention sensor further is to group the plurality of TCP packets into packet flows and communication sessions, store information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to one or more of the packet flow descriptors, search for a network attack identifier, in the TCP stream, based on the packet flow descriptors and the communication sessions associated with the TCP stream.

Copeland is relied on for the teaching of the network intrusion detection and prevention sensor further is to group the plurality of TCP packets into packet flows and communication sessions (***Copeland, paragraphs 0039; 0050***), store information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to one or more of the packet flow descriptors (***Copeland, paragraph 0050, "The flow data structure stores collected flow information such as IP addresses. The flow data structure also stores time and other related packet information from the packet header."*** **Applicants does not clearly define about the communication session in the claim but disclose in the specification (Para 0094) that the packet flow descriptors addressed by each key consist of information about each specific packet flow, each packet flow is associated to a session, such as TELNET session, FTP session, and HTTP session. It is well-known and can be found any network textbook that packet header contains** protocol information [on networks that carry multiple types of information, the protocol defines what type of packet is being transmitted: e-mail (SMTP), Web page (HTTP), streaming video (RTSP)]. However, Copeland further teaches in paragraph 0034, 0038, data flow contains data packet that can include FTP, SMTP, HTTP communications. It is obvious that each packet flow in Copeland points to one of the communication session and each of the communication session points to one or more packet flow), search for a network attack identifier, in the TCP stream, based on the packet flow descriptors and the communication sessions associated with the TCP stream (***Copeland, paragraphs 0051, 005, 0081-0083, 0172***).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of grouping the plurality of TCP packets into packet flows and sessions in the

system of Gleichauf, Nikander and Trcka, as Copeland teaches so as to effectively determine if the traffic data appears to be legitimate or possible suspicious activity.

**Regarding claim 43**, (currently amended) Gleichauf further teaches the system of claim 42, where the network intrusion detection and prevention sensor is located within a firewall (***Gleichauf, col. 4, lines 47-49***).

**Regarding claim 44**, (currently amended) Gleichauf further teaches the system of claim 42, where the network intrusion detection and prevention sensor is located outside a firewall (***Gleichauf, col. 5, lines 24-27***).

**Regarding claim 45**, (currently amended) Gleichauf further teaches the system of claim 42, where the network intrusion detection and prevention sensor further is to: reconstruct on IP defragmentation software module for reconstructing a plurality of packet fragments into the plurality of TCP packets (***Gleichauf, col. 6, lines 39-40***).

**Regarding claim 55**, (currently amended) Gleichauf further teaches the system of claim 42, where the central management server further is to comprise:

collect a plurality of security logs and alarms recording information about the security breach breaches found in the TCP stream (***Gleichauf, col. 7, lines 1-5***); store a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented (***Gleichauf, col. 5, lines 33-42***); and distribute a routine for distributing the network security policy to the network intrusion detection and prevention sensor (***Gleichauf, Fig. 2, element 20***).

**Regarding claim 56**, (currently amended) Gleichauf-Nikander-Copeland-Trcka further teaches the system of claim 42, where the graphical user interface further is to comprises: display

network security information to network security administrators; display status information regarding the network intrusion detection and prevention sensor; and specify a routine for specifying a network security policy (***Copeland, page 11, paragraph [0182]***).

***Claims 57-58, 60-63, and 65-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) in view of Nikander et al. (6,253,321), and in further view of Copeland, III (2003/0105976)***

**Regarding claim 57,** (currently amended) Gleichauf discloses a network intrusion detection and prevention sensor for detecting and preventing network security breaches at a network gateway, the network intrusion detection and prevention sensor comprising (***e.g. col. 2, lines 42-47, "a method and system for adaptive network security using intelligent packet analysis"; fig. 2,3***):

a TCP reassembly software module to reassemble a plurality of TCP packets into a TCP stream (***i.e. TCP stream reassembly, col. 6, lines 39-40, to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer***); a software module to inspect the TCP stream to detect information indicative of a security breach (***e.g. col. 3, lines 1-4***), where, when the network intrusion and detection sensor is to inspect the TCP stream, the network intrusion and detection sensor further is to wherein inspecting the TCP stream to detect information indicative of a security breach (***e.g. col. 2, lines 50-55***)comprises: storing a plurality of protocol specifications supported by a network in a protocol database, and querying the protocol database to determine

whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (***col. 6, lines 31-33; col. 8, lines 20-35***);

Gleichauf (6,324,656) also discloses inspecting the TCP stream to detect information indicative of a security breach comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (***Fig. 3B; col. 6, lines 32 – col. 7, line 5***).

Gleichauf does not explicitly disclose drop / a software module to drop a TCP packet from the TCP stream if the TCP stream contains information indicative of the security breach; and forward / a software module to forward a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of the security breach;

Nikander is relied on for the teaching of a software module to drop a TCP packet from the TCP stream if the TCP stream contains information indicative of the security breach; and a software module to forward a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of the security breach (***Nikander, col. 4, lines 41-45***);

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf (6,499,107 and 6,324,656), Nikander do not specifically disclose a flow manager software module to group a / group the plurality of TCP packets into packet flows and communication sessions, store information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to one or more of the packet flow descriptors, a software module to search for a network attack identifier, in the TCP stream, based on the packet flow descriptors and the communication sessions associated with the TCP stream.

Copeland is relied on for the teaching of the network intrusion detection and prevention sensor further is to group the plurality of TCP packets into packet flows and communication sessions (***Copeland, paragraphs 0039; 0050***), store information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to one or more of the packet flow descriptors (***Copeland, paragraph 0050, "The flow data structure stores collected flow information such as IP addresses. The flow data structure also stores time and other related packet information from the packet header."*** **Applicants does not clearly define about the communication session in the claim but disclose in the specification (Para 0094) that the packet flow descriptors addressed by each key consist of information about each specific packet flow, each packet flow is associated to a session, such as TELNET session, FTP session, and HTTP session. It is well-known and can be found any network textbook that packet header contains** protocol information [on networks that carry multiple types of information, the protocol defines what type of packet is being transmitted: e-mail (SMTP), Web page (HTTP), streaming video (RTSP)]. However, Copeland further teaches in paragraph 0034, 0038, data flow contains data packet that can

include FTP, SMTP, HTTP communications. It is obvious that each packet flow in Copeland points to one of the communication session and each of the communication session points to one or more packet flow), search for a network attack identifier, in the TCP stream, based on the packet flow descriptors and the communication sessions associated with the TCP stream (***Copeland, paragraphs 0051, 005, 0081-0083, 0172***).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of grouping the plurality of TCP packets into packet flows and sessions in the system of Gleichauf and Nikander, as Copeland teaches so as to effectively determine if the traffic data appears to be legitimate or possible suspicious activity.

**Regarding claim 58**, (currently amended) Gleichauf further teaches the network intrusion detection and prevention sensor of claim 57, further comprising : an IP defragmentation software module to reconstruct_a plurality of packet fragments into the plurality of TCP packets (***Gleichauf, col. 6, lines 39-40***).

**Regarding claim 60, 63**, (currently amended) Gleichauf further teaches the network intrusion detection and prevention sensor of claim 57, where the network intrusion detection and prevention sensor is controlled by a network security policy specifying network traffic to inspect and a plurality of network attacks to be detected and prevented / where the security policy is stored by and distributed to the network intrusion detection and prevention sensor by a central management server (***Gleichauf, col. 5, lines 33-42***).

**Regarding claim 61**, (currently amended) Gleichauf-Nikander-Copeland further teaches the network intrusion detection and prevention sensor of claim 60, where the network security

policy is defined by a network security administrator using a graphical user interface associated with the network intrusion detection and prevention sensor (***Copeland, page 11, paragraph [0182]***).

**Regarding claim 62**, (currently amended) Gleichauf-Nikander-Copeland further teaches the network intrusion detection and prevention sensor of claim 61, where the graphical user interface is to: display network security information to network security administrators; display status information regarding the network intrusion detection and prevention sensor; and specify a the network security policy (***Copeland, page 11, paragraph [0182]***).

**Regarding claim 65**, (currently amended) Gleichauf further teaches the network intrusion detection and prevention sensor of claim 57, where the software module to inspect the TCP stream according to the packet flows and the sessions further comprises a protocol anomaly detection software module (***Gleichauf, col. 6, lines 36-42***).

**Regarding claim 66**, (currently amended) Gleichauf discloses the network intrusion detection and prevention sensor of claim 57, where the software module to inspect for inspecting the TCP stream based on according to the packet flows and the sessions further comprises a stateful signature detection software module (***Gleichauf, col. 6, lines 45-52***).

## *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD RAHMAN whose telephone number is (571)270-7471. The examiner can normally be reached on Monday-Friday (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M.L.R./
Examiner, Art Unit 2438

/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 2438